EXHIBIT 3

Date of Hearing: June 28, 2005

ASSEMBLY COMMITTEE ON JUDICIARY
Dave Jones, Chair
SB 355 (Murray) - As Amended: June 15, 2005

As Proposed To Be Amended

SENATE VOTE : 37-2

SUBJECT : INTERNET SECURITY: ANTI-PHISHING ACT OF 2005

KEY ISSUE : SHOULD THE LEGISLATURE MAKE IT UNLAWFUL FOR A PERSON TO FALSELY IMPERSONATE ONLINE A LEGITIMATE BUSINESS IN ORDER TO ACQUIRE THE PERSONAL AND FINANCIAL INFORMATION OF UNSUSPECTING CONSUMERS?

SYNOPSIS

This bill would enact the Anti-Phishing Act of 2005. As explained by the bill's supporters, "Phishing involves the theft of passwords, account information, and other personal data through the deceptive distribution of e-mail messages designed to look like those of legitimate businesses or government agencies." Unsuspecting consumers who provide their personal information expose themselves to identity theft and other unlawful activity. This measure would make phishing unlawful and would provide for a cause of action against violators of the Anti-Phishing Act. Supporters state that the bill is critical in addressing the rapidly expanding phishing problem. The bill is unopposed.

SUMMARY : Establishes the Anti-Phishing Act of 2005, which makes it illegal for anyone to request a consumer to provide personal information by using e-mail, Web sites, or the Internet to impersonate a legitimate online business. Specifically, this bill :

1)Provides that it is unlawful for a person to use a Web page, email, or the Internet to misrepresent that he or she is an online business and solicit or induce another person to provide his or her personal information without the authority or approval of the online business.

2)Provides that the following persons may bring an action

against a person who violates the Anti-Phishing Act:

a) A person who: i) is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark; and, ii) is adversely affected by a violation of the Act;

b) An individual who is adversely affected by a violation of the provisions of the Act against a person who has directly violated it; and

c) The Attorney General or a district attorney.

3)Designates specific available remedies, including the maximum amount of available damages; and provides that a court may increase the amount of damages and/or award attorney's fees to a prevailing plaintiff.

EXISTING LAW :

1)Makes fraud, in general, actionable where the following has been established: 1) a misrepresentation; 2) knowledge of falsity; 3) intent to defraud, i.e., to induce reliance; 4) justifiable reliance; and 5) resulting damage. (Robinson Helicopter Co., Inc. v. Dana Corp. (2004) 34 Cal. 4th 979, 990.)

2)Provides that an attorney general or district attorney can seek an injunction and civil penalties of up to $2,500 per instance for any unlawful business act or practice; and an individual may seek an injunction for an unlawful business act or practice if he or she suffered an injury in fact and lost money or property as a result. (Bus. & Prof. Code Sections 17200, 17204, 17206.)

FISCAL EFFECT : As currently in print, this bill is keyed fiscal.

COMMENTS : This bill would make it illegal for anyone to try to fraudulently induce a consumer to provide personal information

online by impersonating a legitimate business (i.e. phishing). "Phishing" is a widespread technique for obtaining personal information, and is used to facilitate identity theft and other crimes. Phishers use fraudulent emails or Web sites to trick consumers into providing personal information, such as bank

account numbers and social security numbers, to what is believed to be a legitimate company.

The author's office explains, "Customers often receive a legitimate looking email that appears to be from their bank or [a] retailer with whom they do business. The consumer is often told via e-mail that a review of their account found 'unusual activity' and directs them to a phony website where they are compelled to provide personal information such as their name, account number and other relevant data. Criminals have become very good at mimicking legitimate emails and setting up identical Web sites."

The author's office states, "According to the FBI and the Internet Crime Complaint Center, 78% of all criminal 'phishers' are located in the United States. Of these, 15% of all phishing scams originate in California, the most in the nation. In 2004 alone, there were over 100,000 reports of this fraud with over 76,000 consumers losing money. In reported cases alone, consumers lost over $193 million in 2003 and 2004. The California Alliance for Consumer Protection notes it has received numerous complaints in recent weeks from consumers who filled out forms on false 'eBay web pages' with their personal information, thinking that those pages were authentic."

The Computing Technology Industry Association (CompTIA) states, "Billions of dollars of Californian commerce, jobs and productivity gains are tied to the spread of Internet commerce and communications. Confidence in the integrity of personal information transmitted via the Internet remains an integral part of the medium's development. However, recent independent studies, polls and national news reports reveal that phishing is greatly undermining that confidence, phishing tops the concerns of many inside and outside of the IT industry as potentially hobbling the Internet's exciting growth."

Microsoft states it is important to enact legislation to combat the threat of phishing, in addition to using other tools such as technology innovation, targeted enforcement, and user education. Microsoft contends that the "[s]trong laws and adequate enforcement" provided by SB 355 will be critical to addressing the phishing problem. Similarly, CompTIA notes that this bill "puts real 'teeth'" into its prohibitions by making each separate violation punishable by $500,000 in damages, and tripling damages where a pattern of phishing has been

established.

The author has agreed to make a technical amendment to the bill to clarify that the bill applies whenever a person or entity misrepresents itself to be any business, not just an "online business." According to the author, many phishers represent themselves to be legitimate businesses that may conduct transactions online, but are not exclusively online businesses. Therefore, the author makes the following technical amendment:

Page 3, line 1 and line 2, delete "online".

REGISTERED SUPPORT / OPPOSITION :

Support

California Alliance for Consumer Protection
CompTIA
Microsoft
TechNet

Opposition

None on File

Analysis Prepared by : Elizabeth Linton / JUD. / (916) 319-2334